LEGIBILITY NOTICE

A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

LA-UR-87-1952

LA-UR--87-1952

DE87 011783

TITLE THE R&D/OPERATIONAL MC&A INTERFACE

AUTHOR(S) JAMES P. SHIPLEY

SUBMITTED TO INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT

DISCLAIMER

Los Alamos Los Alamos National Laboratory
Los Alamos, New Mexico 87545

THE R&D/OPERATIONAL MC&A INTERFACE

J. P. Shipley
Los Alamos National Laboratory
Los Alamos, NM USA

ABSTRACT

Improvements in our ability to do materials control and accounting (MC&A) have been steady since the beginning of the nuclear age and the appearance of processes and facilities for handling nuclear materials. The motivation for these improvements has not been just safeguards: the desire for better process control also has played a major role, and the emergence of technology focused on the problems of MC&A has made it possible to pursue such improvements. However, it is a continuing challenge to match the needs of the operational MC&A elements with the capabilities and resources of the R&D community.

In the last couple of years this challenge has been addressed very visibly by the DOE's Project Cerberus R&D Committee, which has devised a procedure to encourage closer interactions between the operations and R&D elements. In the particular case of Los Alamos, we have recently concluded the efforts of the Nuclear Materials Management and Safeguards Task Force, which made strong recommendations about the need for close internal cooperation. The issues associated with these activities and the specific means for addressing them, will be of surpassing interest for the future of safeguards.

INTRODUCTION

The history of nuclear materials production is inextricably bound up with that of materials control and accounting (MC&A) for the simple reason that materials accounting has always been a vital part of nuclear materials process control. The fact that a substantial safeguards R&D program exists today, and that it has the current character, is evidence that MC&A is an important safeguards element, especially in addressing the insider threat, that MC&A technology and its application are complex matters requiring further development, and that MC&A requirements are evolving. The changing nature of safeguards is highlighted by examining the history (see for example the paper *The Evolution of Safeguards Systems Design*[1]).

While it is true that MC&A serves both the needs of process control and safeguards, the reasons why are somewhat different in the two cases[2]. This means that the technical requirements on MC&A

devices and systems also are different. For example, process control relies on measurements of materials and process parameters that need only be precise enough to minimize short-term fluctuations in process operation and product quality. Longer term measurement errors, such as calibration drifts or biases, tend to be less important as long as they are not too large and are relatively constant. On the other hand, for materials accounting, longer term errors, especially for measurements of transfers between materials balance areas (MBAS), tend to be most important because of the cumulative nature of inventory differences (IDS). The precisions of these measurements are certainly of interest, but less so because the associated ID uncertainty component accumulates more slowly than does the component caused by the long-term errors.

The technology needed to satisfy both sets of requirements is not simple, yet it must be accessible to those who have to do both process control and operational MC&A. Therefore, in this paper we examine how that is accomplished through the joint efforts of the R&D and operational MC&A community, and we make some suggestions for improvements.

ORGANIZATIONAL STRUCTURE

Figure 1 shows the structure of DOE/Defense programs relevant to the nuclear weapons complex and its safeguards and security activities. The organization is largely vertical with each facility reporting through its cognizant Field Office to Headquarters (HQ). The programmatic offices at HQ (e.g., Military Applications or Nuclear Materials Production) generally have a counterpart in each Field Office. The Safeguards and Security operations element services both weapons and production, but generally reports to a different section of the Field Office, which in turn reports to the Office of Safeguards and Security (OSS) at HQ. The Safeguards and Security R&D programs report directly to OSS, although there is substantial interaction with the Field Office Safeguards and Security unit. The R&D program interfaces directly at the operating levels of the weapons, production, and safeguards and security elements.

The Office of Safeguards and Security has the responsibility to set standards and criteria, promulgated through the issuance of DOE Orders, to develop Orders that encourage and ensure an appropriate level of safeguards and security for the DOE complex, and provide the basic know-how for carrying out those Orders. It is the responsibility of the programmatic offices to implement the DOE Orders and to maintain that level of safeguards and security in the facilities and operations for which they are responsible. Thus, the programmatic offices and their operating contractors perform the MC&A function in accord with guidelines set down by OSS and assisted by the technology made available by OSS through its safeguards and

security R&D program. Therefore, the primary interface issues become

- how to ensure the issuance of good DOE Orders
- how to ensure that the Orders are complied with, and
- who pays for which parts of that compliance.

PROGRAM CREATION

In the interest of addressing the last two of these issues the Project Cerberus R&D committee, chaired by Glenn Hammond of OSS, examined the nature of the Safeguards and Security R&D program over the last two years. As a result of that effort the program has been restructured and redirected, specifically to incorporate the concept of user-need statements[3]. The program has always been driven by the user community, but this step establishes the formal connection and ensures that all elements of the complex have input to the R&D program.

Mere acquisition of the user-need statements is not sufficient. The process of program creation is much more complex, as shown in Fig. 2[4]. In fact the process is even more complicated than is shown in the Figure. For example, the raw user requests coming from the operating contractors generally are not suitable as direct R&D requirements. The user requests are almost always very strongly focused on specific problems. If a solution already exists, then it should not be pursued under the R&D program, but as a part of safeguards implementation. If a solution does not exist, then to take maximum advantage of limited R&D resources, the body of user requests should be examined to see if an R&D effort could serve more than one need. Sometimes, the requests are so focused as to overspecify the problem, and thus constrain the solution, when, in fact, a more common solution applicable to several areas in the DOE complex might work as well and be less costly overall. Occasionally, requests are made for capabilities that would exceed an appropriate level of safeguards (e.g., measuring a low-level waste stream to 0.1 percent) or that fail to recognize that MC&A technology is evolving.

Consequently, a loop not shown in Fig. 2, but one that is absolutely essential to an effective R&D program, is from the Centers of Excellence back to the user community on an on-going basis. If the Centers of Excellence waited for the user requests to come in rolling before structuring their program, the real user needs would seldom be discovered, and certainly not in a timely fashion. Another way of saying the same thing is that day-to-day interaction and cooperation at the working level among the operators, users, and developers is a fundamental requisite to improving safeguards.

FUNDING ARRANGEMENTS

The situation here is very simple: OSS pays for R&D, the programmatic office pays for implementation. The only difficulty is determining which is which. Certainly, OSS provides funds for generic R&D that covers several problems in the complex. Site-specific implementation is paid for out of DOE programmatic funds. However, there is a gray area of field assistance and so called site-specific R&D that always comes into question. Furthermore, emerging safeguards technology needs to be demonstrated, tested, and evaluated in operating facilities to ascertain that it can do the safeguards job effectively. The situation is represented in Fig. 3.

In the past, the relative contributions of OSS and the programmatic offices has been negotiated. However, the OSS program is highly leveraged, being approximately one percent of the overall defense budget, with only 10 percent of the amount spent by the programmatic offices on safeguards and security matters. This latter figure derives from the DOE safeguards and security crosscut budget, which is not a budget but a compilation of programmatic funding expenditures related to safeguards and security. Historically, most of that expenditures have been on security.

OPERATION OF THE INTERFACE

At the working level, the interface functions on a daily one on-one, technical basis. By virtue of these contacts, safeguards developers become aware of specific problems, the solutions to which may have had applications at other facilities in the complex. Oftentimes process, operational MC&A, and R&D personnel are shared so that the special problems of each area can be appreciated by those in the other areas. These days, planning for new facility and their related safeguards requirements is more and more being done early in the design process so that safeguards considerations can be factored in at lower costs and probably more effectively. Also, the scope of the safeguards requirements, and therefore planning for increased resources can be done more accurately. Likewise, new DOE Orders are beginning to incorporate the interest and capabilities of all elements of the community, which is important in obtaining willing compliance with them and in making them achievable.

At Los Alamos we have formalized a concept of the Safeguards Implementation Project Team, both to help our own in-house safeguards upgrades activities, and to continue supporting improvements around the complex[8]. We have also restructured our safeguards and

security R&D program along the lines shown in Fig. 4. Our program has four major tasks:

- Task 1: Science and Technology Base
- Task 2: Basic Systems Design and Integration
- Task 3: Onsite Test and Evaluation
- Task 4: International Safeguards.

We undertake projects in Tasks 1, 2, and 3 according to the distillation of R&D requirements from the user-need statements mentioned previously.

POSSIBLE IMPROVEMENTS

The user interface between operations and R&D has improved substantially in the past few years, but there are still areas where we could do even better. The following are a few suggestions.

Attitudes--Sometimes safeguards have been brushed aside by those operating the processes by saying, "That's not in my job description." Well, I think safeguards has to be made a part of their job descriptions. Likewise, the programs, and individuals responsible for them, that comprise the nuclear weapons complex must consider safeguards and security as an integral part of their operations, just like safety, for example.

Organization--The current organizational structure is fine except that there need to be closer ties among operational MC&A, the process line, and safeguards R&D. In keeping with the concept under attitudes, the process operators need to be doing their own MC&A. If there is a separate operational MC&A element as an organizational unit, it should be assisting the process operators, not doing it for them. We have a paradigm for this arrangement in the IAEA. There, each State does its own materials accounting, which is then verified by the IAEA inspectors. The IAEA does not do the materials accounting for the States.

Effectiveness Evaluation--We need a logical method of evaluating the effectiveness of various safeguards and security techniques and approaches as a means of making rational decisions about resource allocations. These decisions should be made on the basis of an assessment of risk, which I define as follows:

$$\text{Risk} = \text{Threat} \times \text{Vulnerabilities} \times \text{Consequences}.$$

This assessment need not be highly formalistic, nor even necessarily quantitative. The point is that safeguards decisions should not be based solely on someone's concept of any of the three components of risk. A possible procedure for doing the assessment is depicted in Fig. 5. Such a logic will form the underpinnings for a way of alleviating the concerns of Congress and the public. The emerging Master Safeguards and Security Agreements being developed for each site are a first step in the right direction.

Funding--A method of deciding, in a mutually satisfactory and supportive way, the relative contributions of OSS and the programmatic offices to safeguards and security upgrades must be devised. Again, this process will become easier as attitudes evolve toward understanding that safeguards is our common concern.

REFERENCES

1. J. P. Shipley, E. L. Christensen, and R. J. Dietz, "The Evolution of Safeguards Systems Design", Proceedings of ANS/INMM Topical Conference on Measurement Technology for Safeguards and Materials Control. Kiawah Island, South Carolina, November 26-29, 1979.

2. J. P. Shipley " The Bridge Between Safeguards and Process Operations" 1982 National American Institute of Chemical Engineers meeting, Orlando, Florida, February 1982.

3. Safeguards and Security R&D Directory and Long Range Plan, FY 1987 - 1992. USDOE/OSS, October 1986.

4. Office of Safeguards and Security R&D Program Planning Guide prepared by International Energy Associates, Limited. February 19, 1986.

5. Report of the Nuclear Materials Management and Safeguards Task Force, Los Alamos National Laboratory internal document, November 1986.